United States Department of Agriculture
Grain Inspection, Packers and Stockyards Administration

Program Notice GIPSA PN-04-07 02/20/04

CYBER SECURITY RISK MANAGEMENT

1. PURPOSE

This program notice establishes the Grain Inspection, Packers and Stockyards Administration (GIPSA) cyber security risk management program.

2. EFFECTIVE DATE

This action is effective upon receipt.

3. BACKGROUND

The current heightened sense of national alert and the Administration's focus on the security of Federal Information Technology (IT) assets requires that all government agencies, including GIPSA, take immediate action to secure their IT systems. In addition, the General Accounting Office (GAO) has issued reports over the past several years that describe persistent computer security weaknesses in the federal sector which support this requirement. These pervasive weaknesses introduce risks that could allow malicious or unintentionally dangerous users to read, modify, delete or otherwise damage information or disrupt operations. The reasons or motivations of the attacker could include curiosity, criminal activities, sabotage, espionage or terrorism and could seriously affect GIPSA's mission.

Protection of information assets and maintaining the availability, integrity and confidentiality of GIPSA's information technology assets and telecommunications resources are vital in meeting GIPSA's program delivery requirements. Implementation of security measures such as a cyber security risk management program, effective security controls, certification and accreditation of IT systems and updated security plans are vital components in our response to this situation.

Recently, the Department's Office of the Chief Information Officers (OCIO) directed all USDA agencies to implement a structured approach in assessing risk to USDA IT assets, including agency-owned assets. Such programs are a key component to implementation of appropriate security controls, and the certification and accreditation of agency IT systems.

4. POLICY

GIPSA will periodically conduct formal Risk Assessments (RA) of all GIPSA-owned or controlled IT systems. RAs will be conducted in accordance with the USDA Risk Assessment Methodology found in USDA Publication CS-031, "Security Guidance Regarding Risk Assessment Methodology." A formal system risk analysis will be conducted every three years and when a major change is made in a GIPSA system. Major changes are defined as modifications to the system that affect the security controls and which render the system vulnerable to compromise or intrusion.

Agency managers will include the cost for IT system mitigations in budgetary planning and prepare a business case to ensure that funding is available to implement protection against identified vulnerabilities.

5. DEFINITIONS

a. Asset: A major application, general support system, high impact program, physical plant, mission critical system or logically related group of systems

b. Automated Information System: Assembly of electronic equipment, hardware, software and firmware configured to collect, create, communicate, disseminate, process, store, and control data or information.

c. IT Related Risk: The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) particular information system vulnerability and (2) the resulting impact if this should occur.

d. Risk Assessment (RA): The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate the impact.

e. Risk Management (RM): An ongoing process of assessing the risks to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk. Simply stated, RM is a total process of identifying, controlling, and mitigating information system related risks.

6. RESPONSIBILITIES

a. GIPSA Chief Information Officer(CIO) will:

(1) Actively implement the GIPSA Cyber Security Risk Management Program, including the use of the USDA Risk Assessment Methodology

(see USDA Cyber Security Guidance Regarding Risk Assessment Methodology, CS-031, Table 1 at http://www.ocionet.usda.gov/ocio/cyber_sec/policy.html), to conduct assessments of all IT systems and to implement risk mitigations;

(2) Ensure the all GIPSA IT professionals understand their role in the risk assessment process, with special emphasis on system owners, developers, security officers and system administrators;

(3) Use a formal System Development Life Cycle (SDLC) and Configuration Management (CM) approach in the management of IT systems to support the internal Risk Assessment Program;

(4) Prepare a quarterly report to USDA, Cyber Security (CS) for Federal Information Security Management Act of 2002 (FISMA) reporting of RA's performed for systems to include: proposed RA dates or a summary of major findings with mitigations and implementation timeframes signed by the CIO;

(5) Develop and submit an IT budget, funding requests and business cases to implement necessary risk mitigations on agency systems, as appropriate;

(6) Update System Security Plans to include RA date, major findings, mitigations and timeframes for action;

(7) Document residual risk in a Residual Risk Statement; and

(8) Take action to request a formal waiver for systems that do not comply with this policy.

b. GIPSA Information System Security Program Managers (ISSPM) will:

(1) Stay abreast of GIPSA and USDA policy and agency roles;

(2) Support the implementation of the GIPSA internal Risk Management Program;

(3) Participate in system risk assessments and document preparation, as required;

(4) Involve system Designated Approving Authority's (DAA) in all aspects of the Risk assessment process, only the DAA can accept residual risk on a system.

(5) Update System Security Plans with Risk Assessment information and participate in the development of risk mitigations and costs;

(6) Participate in the development and submission of funding requests for mitigations, as required; and

(7) Review and monitor all agency IT systems to ensure RAs are conducted as required by this policy; report non-compliant systems to the agency CIO and Cyber Security on a quarterly basis unless the system is under an approved formal waiver.

7. QUESTIONS

Direct questions to the GIPSA Information Systems Security Program at (202) 720-1741.

/s/ Donna Reifschneider

Donna Reifschneider
Administrator